MA294 Lecture

Timothy Kohl

Boston University

January 23, 2024

$\mathbb{Z}_m$ the integers mod m - "$\mathbb{Z}$ mod m"

Recall that for a given modulus $m > 1$ that any integer a is congruent to exactly one $r \in \{0, \ldots, m-1\}$ because, by the division algorithm

$$a = q \cdot m + r$$

for unique q, r, where $r \in \{0, 1, \ldots, m-1\}$.

With this and the arithmetic properties of $\equiv$ we just proved, one can define a system of numbers that is based on the integers $\mathbb{Z}$ but is finite in size.

Definition

The set of integers mod m denoted $\mathbb{Z}_m$ is the set of distinct equivalence classes

$$\{[0], [1], \ldots, [m-1]\}$$

with respect to the equivalence relation of congruence mod m.

For example $\mathbb{Z}_3 = \{[0], [1], [2]\}$ since $\mathbb{Z} = [0] \cup [1] \cup [2]$.

Bear in mind that we are treating these infinite sets $[a]$ as though they are individual entities, which they are since each equivalence class is different than another,but we can treat $\mathbb{Z}_m$ as a finite set since there are only finitely many equivalence classes in $\mathbb{Z}_m$.

Later on we will take this even further by dropping the '[]' around the $[r]$.

The facts we proved earlier show how the congruence relation is 'compatible' with addition and multiplication.

With this in mind we define the following addition and multiplication operations on the set $\mathbb{Z}_m$.

Definition

If $[x], [y] \in \mathbb{Z}_m$ then $[x] + [y] = [x + y]$ and $[x] \cdot [y] = [xy]$.

The key fact(s) to be verified is that this operation is 'closed' namely that $[x] + [y] \in \mathbb{Z}_m$ and $[x] \cdot [y] \in \mathbb{Z}_m$.

In lieu of a formal proof, let us consider some examples which illustrate this very clearly.

Example: $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$.

$[2] + [4] = [2 + 4] = [6] = [1]$ since $6 \equiv 1 \ (mod \ 5)$

$[4] + [1] = [4 + 1] = [5] = [0]$

$[2] + [2] = [2 + 2] = [4]$

$[2] + [0] = [2 + 0] = [2]$

$[2] \cdot [4] = [2 \cdot 4] = [8] = [3]$ since $8 \equiv 3 \ (mod \ 5)$

$[3] \cdot [1] = [3 \cdot 1] = [3]$

$[2] \cdot [3] = [2 \cdot 3] = [6] = [1]$

For simplicity, it's easier to write $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ and compute $a + b$ and $a \cdot b$ mod m by computing the appropriate remainders 'mod m'.

Ex: $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$

- $2 + 3 = 5$
- $4 + 3 = 1$
- $5 \cdot 2 = 4$
- $3 \cdot 3 = 3$ (Yes, this can happen.)

Theorem

In $\mathbb{Z}_m$ the operations $+$ and $\cdot$ follow the following rules.
Let $a, b, c \in \mathbb{Z}_m$

- *(1) $a + b = b + a$ [Commutativity]*
- *(2) $a \cdot b = b \cdot a$ [Commutativity]*
- *(3) $(a + b) + c = a + (b + c)$ [Associativity]*
- *(4) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ [Associativity]*
- *(5) $a + 0 = a$ [Additive Identity]*
- *(6) $a \cdot 1 = a$ [Multiplicative Identity]*
- *(7) $a(b + c) = ab + ac$ [Distributive Law]*
- *(8) For each $a \in \mathbb{Z}_m$, there exists $b \in \mathbb{Z}_m$ such that $a + b = 0$. [Additive Inverses]*

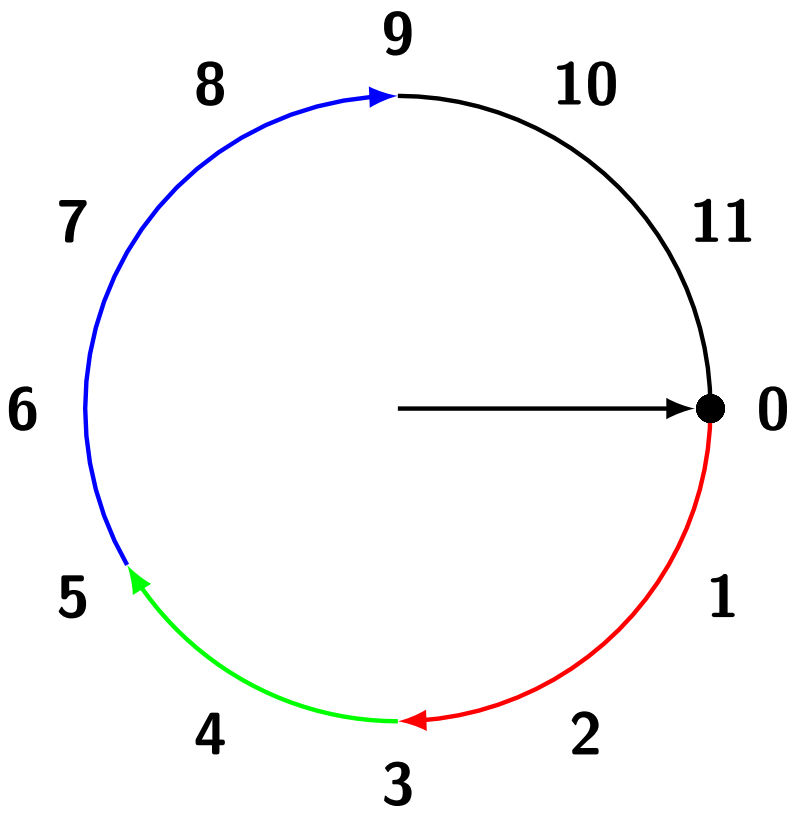
Proof.

(Sketch) (5),(6) If $[a] \in \mathbb{Z}_m$ then $[a] + [0] = [a + 0] = [a]$, and similarly $[a] \cdot [1] = [a \cdot 1] = [a]$.

(8) If $a \in \mathbb{Z}_m$ then if we let $b = m - a$ then $b \in \mathbb{Z}_m$ and obviously $[a] + [b] = [a] + [m - a] = [a + m - a] = [m] = [0]$ in $\mathbb{Z}_m$.

So, for we may define $-a$ to be $m - a$ and observe that $a + (-a) = 0$. □

As to the associativity of addition, $(a+b)+c = a+(b+c)$ we invoke an image which really conveys why the parentheses don't matter.



Here, if we represent a number in $\mathbb{Z}_{12}$ as clockwise rotation, and the sum of two numbers as the composition of two rotations then it's clear why, for example $(3+2)+4 = 3+(2+4) = 3+2+4 = 9$.

Recall that if $a \in \mathbb{Z}_m$ there exist $b \in \mathbb{Z}_m$ such that $a + b = 0$, i.e. $b = -a$.

For the multiplication operation, the analogue would be:

$$\text{For each } a \in \mathbb{Z}_m \text{ there exists } b \in \mathbb{Z}_m \text{ such that } a \cdot b = 1$$

The problem is that this is not always the case.

For example, in $\mathbb{Z}_6$, if $a = 2$ then $b \in \mathbb{Z}_6$ would have to have the property that $2b \equiv 1 \ (mod\ 6)$, but observe that for $\mathbb{Z}_6$ we have

- $2 \cdot 0 = 0$
- $2 \cdot 1 = 2$
- $2 \cdot 2 = 4$
- $2 \cdot 3 = 0$
- $2 \cdot 4 = 2$
- $2 \cdot 5 = 4$

So $2b = 1$ is impossible.

However, depending on the modulus m and $a \in \mathbb{Z}_m$ one does have such 'multiplicative inverses'.

Example: In $\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ let $a = 2$ then one may verify that $b = 5$ is such that $ab = 1$, i.e. $2 \cdot 5 = 10 = 1$ in $\mathbb{Z}_9$, i.e. We may write $2^{-1} = 5$ in $\mathbb{Z}_9$.

Definition

An element $r \in \mathbb{Z}_m$ is invertible (or a unit mod m) if there is some $x \in \mathbb{Z}_m$ such that $rx = 1$ in $\mathbb{Z}_m$.
In that case, x is called the multiplicative inverse of r and we write $r^{-1} = x$.

Example: Again in $\mathbb{Z}_9$, $4^{-1} = 7$ since $4 \cdot 7 = 28 \equiv 1 \ (mod\ 9)$.

Note, in contrast, that 6^{-1} does not exist in $\mathbb{Z}_9$.Why?

Theorem

The only $r \in \mathbb{Z}_m$ that have inverses are those for which $gcd(r, m) = 1$, that is 'r is co-prime to m'.

Recall that $gcd(r, m)$ means 'greatest common divisor of r and m'.

Proof.

Suppose $rx = 1$ in $\mathbb{Z}_m$ then we have

$$rx - 1 = qm$$

for some q.

Well then $rx - qm = 1$ so if $d|r$ and $d|m$ (i.e. d divides r and m) then $r = da$ for some a, and $m = db$ for some b.

But then $rx - qm = dax - qdb = d(ax - qb)$ but $rx - qm = 1$ do that $d|1$!

So the only conclusion is that $d = 1$, i.e. the only common divisor of r and m is 1. For the converse we use the following FACT known as *Bezout's Identity* which is that, if $gcd(r, m) = 1$ then there exists a, b such that $ar + bm = 1$.

As such, $ar - 1 = (-b)m$ which means $ar \equiv 1 \ (mod \ m)$ i.e. $r^{-1} = a$, that is, r is invertible. □

The invertible elements of $\mathbb{Z}_m$ gives rise to this.

Definition

For $m > 1$ the units mod m is

$$U(m) = \{r \in \mathbb{Z}_m \mid gcd(r, m) = 1\}$$

which is precisely the set of invertible elements of $\mathbb{Z}_m$.

Note, $0 \notin U(m)$ for any m and the size of $U(m)$ (as a set) is what is known as

$$\phi(m) = \text{ Euler's Function, or Totient}$$

and it is interesting to consider the value of $\phi(m)$.

Example:

- $\mathbb{Z}_2 = \{0, 1\} \to U(2) = \{1\} \to \phi(2) = 1$
- $\mathbb{Z}_3 = \{0, 1, 2\} \to U(3) = \{1, 2\} \to \phi(3) = 2$
- $\mathbb{Z}_4 = \{0, 1, 2, 3\} \to U(4) = \{1, 3\} \to \phi(4) = 2$
- $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\} \to U(5) = \{1, 2, 3, 4\} \to \phi(5) = 4$
- $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\} \to U(6) = \{1, 5\} \to \phi(6) = 2$
- $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\} \to U(7) = \{1, 2, 3, 4, 5, 6\} \to \phi(7) = 6$
- $\mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\} \to U(8) = \{1, 3, 5, 7\} \to \phi(8) = 4$
- $\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\} \to U(9) = \{1, 2, 4, 5, 7, 8\} \to \phi(9) = 6$

One observation we can make about the ϕ function is that if m is prime then $\phi(m) = m - 1$.

The reason for this is that if m is prime then any $r < m$ is never a divisor since m is prime.

But before developing further properties of ϕ we need some to make some observations about $U(m)$.

- If $r, s \in U(m)$ then $rs \in U(m)$.(Why? Well $gcd(r, m) = 1$ and $gcd(s, m) = 1$ implies $gcd(rs, m) = 1$.)
- $1 \in U(m)$ for all m (obviously, since $1 \cdot 1 = 1$ so $1^{-1} = 1$)
- If $r \in U(m)$ then $r^{-1} \in U(m)$.[Exercise]

These properties, as we'll discuss later on, make $U(m)$ into what we know as a *group*.

One important property of ϕ is this.

Proposition

If $gcd(r, s) = 1$ *then* $\phi(rs) = \phi(r)\phi(s)$.

Proof.

(Sketch)The basic idea is to consider the function $\rho : U(rs) \to U(r) \times U(s)$ defined by $\rho(x) = (x^*, x^{**})$ where x^* is the remainder when x is divided by r and x^{**} is the remainder when x is divided by s.

As $gcd(r, s) = 1$ then one can show that this map is 1-1 and onto, so that

$$|U(rs)| = |U(r) \times U(s)| = |U(r)| \cdot |U(s)|$$

namely that $\phi(rs) = \phi(r)\phi(s)$. □

We should note that this not necessarily true if r and s are not relatively prime.

We have another very important property of the ϕ function, in particular to its application to modern cryptography.

Theorem

If $a \in U(m)$ then $a^{\phi(m)} \equiv 1 \pmod{m}$. (Euler - 1763)

Proof.

(Sketch) If $U(m) = \{a_1, a_2, \ldots, a_{\phi(m)}\}$ where, without loss of generality $a_1 = 1$ then for $a \in U(m)$ consider

$$\{aa_1, aa_2, \ldots, aa_{\phi(m)}\}$$

and observe that, since $a \in U(m)$ then $aa_i = aa_j$ implies $a^{-1}aa_i = a^{-1}aa_j$, that is $(a^{-1}a)a_i = (a^{-1}a)a_j$ and since $a^{-1}a = 1$ then this implies that $a_i = a_j$. As such, $\{aa_1, aa_2, \ldots, aa_{\phi(m)}\}$ is a rearrangement (or permutation) of $\{a_1, a_2, \ldots, a_{\phi(m)}\}$ and so

$$aa_1aa_2 \ldots aa_{\phi(m)} = a_1a_2 \cdots a_{\phi(m)}$$

namely $a^{\phi(m)}b = b$ where $b = (a_1a_2 \cdots a_{\phi(m)})$ which means

$$a^{\phi(m)}bb^{-1} = bb^{-1}$$

where, of course $bb^{-1} = 1$ so $a^{\phi(m)} = 1$. □

A simpler version of this result is known as Fermat's (Little) Theorem, namely for $m = p$ a prime and $gcd(a, p) = 1$ then $a^{p-1} \equiv 1 \ (mod \ p)$ since $\phi(p) = p - 1$.

As mentioned earlier, Euler's theorem (although a 200+ year old theorem) is at the heart of the RSA (public key) encryption system that is integral to modern electronic commerce and general security online.